On finite simple braces

Jan Okniński
University of Warsaw

Lecce, September 2017

Plan of the talk

1. set theoretic solutions and braces
2. three important results
3. matched products and simple braces
4. asymmetric products and simple braces
5. simple braces of arbitrary derived length
6. some open problems

New results presented in this talk are based on joint work with D. Bachiller, F. Cedó, E. Jespers

- arXiv:1610.00477 (Transactions AMS, to appear)
- arXiv:1705.08493

Set theoretic solutions

Definition

Let X be a nonempty set and $r : X^2 \longrightarrow X^2$ a bijective map. One says that r is a set theoretic solution of the Yang-Baxter equation if it satisfies on X^3 the braid relation

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}$$

where r_{ij} stands for the mapping $X^3 \longrightarrow X^3$ obtained by application of r in the components i, j and identity in the remaining component.
A solution is often denoted by (X, r).

For a solution (X, r), let

$$\sigma_x, \gamma_y : X \longrightarrow X$$

be the maps defined by

$$r(x, y) = (\sigma_x(y), \gamma_y(x)).$$

Definition

A set theoretic solution (X, r) is called:

(1) involutive if $r^2 = \mathrm{id}_{X \times X}$,

(2) non-degenerate if all maps σ_x an γ_y are bijections.

We will only discuss finite non-degenerate involutive solutions.

Braces we introduced by W.Rump as a tool in the study of set theoretic (involutive, non-degenerate) solutions of the Yang-Baxter equation.

Definition

A left brace is a set B with two binary operations, $+$ and $\cdot$ such that $(B,+)$ is an abelian group, $(B,\cdot)$ is a group and
$(*)\quad a\cdot(b+c)+a=a\cdot b+a\cdot c$ for all $a,b,c\in B$.

It is easy to see that in a left brace we have $0=1$.

An example: B is a *trivial left brace* if $(B,+)$ is an abelian group and the operations $+$ and $\cdot$ coincide.

More generally: the class of Jacobson radical rings coincides with the class of *two-sided braces* (symmetric version of condition $(*)$ also holds in B). (If $(B,+,\cdot)$ is a two-sided brace then $(B,+,*)$ is a radical ring, where $a*b=ab-a-b$.)

If B is a left brace then we have an action $\lambda : (B, \cdot) \longrightarrow \mathrm{Aut}(B, +)$ defined by $\lambda(a) = \lambda_a$, where $\lambda_a(b) = ab - a$ for $a, b \in B$. This is called the lambda map of the brace B.

Given an abelian group $(B, +)$ and a map $\lambda : B \longrightarrow \mathrm{Aut}(B, +)$ such that $\lambda_a \circ \lambda_b = \lambda_{a+\lambda_a(b)}$, the rule $a \cdot b = a + \lambda_a(b)$ defines a structure of a left brace $(B, +, \cdot)$. Here $\lambda_a = \lambda(a)$.

Hence, given a lambda map, the structure $(B, +)$ determines $(B, \cdot)$ and vice versa: $a + c = a \cdot \lambda_{a^{-1}}(c)$.

Recently, braces have been discovered in several different mathematical contexts. In particular:

- radical rings,
- regular subgroups of affine groups,
- groups of I-type and Bieberbach groups,
- Hopf-Galois structures,
- quandles and knot theory,
- Garside groups,
- affine structures on Lie groups,
- self distributive structures.

Definition

An ideal of a left brace B is a normal subgroup I of the group $(B, \cdot)$ such that $\lambda_a(b) \in I$ for every $b \in I$ and $a \in B$.

If I is an ideal of B then $a - b = bb^{-1}a - b = \lambda_b(b^{-1}a) \in I$ for $a, b \in I$. Hence, I is a subgroup of the group $(B, +)$. Moreover, B/I has a natural structure of a left brace.

Definition

A left brace $B \neq \{0\}$ is simple if $\{0\}$ and B are the only ideals.

An example: the trivial brace structure on the cyclic group $\mathbb{Z}_p$ of prime order p.

Definition

By the socle of a left brace B we mean the set
$\mathrm{Soc}(B) = \{a \in B | a \cdot b = a + b \text{ for all } b \in B\}$.
(In other words: $\lambda_a = \mathrm{id}_B$ for every $a \in B$.)

Note: $\mathrm{Soc}(B)$ is an ideal and $\mathrm{Soc}(B)$ is a trivial brace.

Definition

Let (X, r) be a solution. Denote by $\mathcal{G}(X, r)$ the subgroup $\langle \sigma_x \mid x \in X \rangle$ of the symmetric group Sym_X.

It can be shown that $\mathcal{G}(X, r)$ and the group $\langle \gamma_x \mid x \in X \rangle$ are conjugate in Sym_X.

Let $G(X, r)$ be the group defined by the presentation

$$\langle X \mid xy = \sigma_x(y)\gamma_y(x) \quad \text{if} \quad r(x, y) = (\sigma_x(y), \gamma_y(x)) \rangle.$$

It is called the structure group of the solution (X, r).

$G(X, r)$ admits a natural structure of left brace, such that its additive group is the free abelian group with basis X and the lambda map is given by: $\lambda_x(y) = \sigma_x(y)$ for all $x, y \in X$.
Then $\mathcal{G}(X, r)$ is a homomorphic image of $G(X, r)$ and it inherits the left brace structure from $\mathcal{G}(X, r)$.

Definition

A group H is called an involutive Yang-Baxter group (IYB-group) if it is isomorphic to $\mathcal{G}(X, r)$ for a solution (X, r) with a finite set X.

Theorem (Bachiller, Cedó, Jespers)

Every left brace determines (constructively) a family of solutions (X, r) of the Yang-Baxter equation such that $\mathcal{G}(X, r) \cong B$ as left braces. Moreover, each solution arises in this way.

The challenging problem: describe all finite left braces.

Strategy:
- describe all finite simple left braces,
- develop a theory of extensions of left braces.

Three important necessary conditions

Theorem (Etingof, Schedler, Soloviev)

The multiplicative group $(B, \cdot)$ of a finite left brace is solvable.

Recall that a Sylow basis of a finite group G is a collection of Sylow subgroups $G_1, \ldots, G_n$ (one for every prime dividing $|G|$) such that $G_i G_j = G_j G_i$ for all i, j. It is known that, if such a system exists then G is solvable (P.Hall).

Let $(B, +) = \prod B_p$, where B_p are the Sylow subgroups. Then B_p are λ_x-invariant for every $x \in B$ (as $\lambda_x \in \mathrm{Aut}(B, +)$) and $a + b = a\lambda_{a^{-1}}(b) = b\lambda_{b^{-1}}(a)$ if $a \in B_p, b \in B_q$.
(Recall that $\lambda_x(y) = xy - x$.)
Thus $B_p + B_q = B_p B_q = B_q B_p$. So B_p are also Sylow subgroups of $(B, \cdot)$, and we get a Sylow basis of $(B, \cdot)$. Hence, $(B, \cdot)$ is solvable.

The original proof was concerned with solvability of the structure groups $G(X, r)$ of solutions of the YB equation. Then the result follows from the correspondence between braces and solutions.

Theorem (Rump)

If B is a finite simple left brace and $|B| = p^n$ for some prime p then $n = 1$ and B is a trivial brace.

Suppose that $n > 1$. Then $pB \subsetneq B$ is closed under all λ-maps. So $pB \subseteq B$ is a "left $(B, \cdot)$-module" via the action:

$$a \cdot x = \lambda_a(x), \quad \text{for} \quad a \in B, z \in B$$

Take any maximal submodule M such that $pB \subseteq M \subseteq B$. Then B/M is a module over the group ring $\mathbb{F}_p[(B, \cdot)]$. But there is only one simple module, which is trivial. Therefore

$$B * B = \{\lambda_a(x) - x : a \in B, x \in B\}_+ \quad \text{(additive closure)}$$

is contained in M. One verifies that $B * B$ is an ideal of B. Simplicity of B implies that $B * B = 0$ (because $B * B \subseteq M \neq B$). Thus, $\lambda_a(x) = x$ for $a \in B, x \in B$. Thus, B is a trivial brace. So, every subgroup of $(B, +)$ is an ideal. It follows that $|B| = p$.

Theorem (Smoktunowicz)

Let B be a finite simple left brace and let $|B| = q^r k$, where q is a prime, $q \nmid k$ and $k \neq 1$. Then

1. *there exists a prime p and a positive integer t such that $q|(p^t - 1)$ and $p^t|k$,*
2. *$|B|$ is not cube-free.*

Let $(B, +) = \prod B_p$, where B_p are the Sylow subgroups. We have seen that this is a Sylow basis $(B, \cdot)$.
For every p we know that B_p is not a normal subgroup of $(B, \cdot)$, because it would be an ideal, while B is a simple brace.
So, for every p there exists a q such that B_p is not a normal subgroup of the multiplicative group $B_p B_q$. Assertion 1) follows by Sylow's theorem.

Suppose $|B|$ is cube-free. Let $p_1 < p_2 < \cdots < p_m$ be all primes dividing $|B|$. Then, by 1),

$$p_m|(p_i - 1) \quad \text{or} \quad p_m|(p_i^2 - 1) \quad \text{for some } i < m.$$

Thus, $p_m = p_{i+1}$ and hence $p_1 = 2, p_m = 3$, so that $m = 2$. Hence $B = B_2 B_3$ and it follows that $|B| = 6, 12, 18$, or 36.

An analysis of each of these cases leads to the conclusion that $\mathrm{Soc}(B) \neq 0$. Since $\mathrm{Soc}(B)$ is an ideal and B is simple, we get that $B = \mathrm{Soc}(B)$, so it is a trivial brace. Then simplicity implies that the order of B is a prime number, a contradiction.

Finite simple left braces - matched product approach

The first examples of finite simple left braces that are non-trivial were constructed by D.Bachiller. Their additive groups are isomorphic to the group $\mathbb{Z}_p \times (\mathbb{Z}_q)^{k(p-1)+1}$ for two primes p, q such that $q|(p-1)$ and k is an arbitrary positive integer.

Definition

We say that I is a left ideal of a left brace B if I is a subgroup of the additive group $(B, +)$ such that $\lambda_a(b) \in I$ for every $a \in B$ and $b \in I$.

Definition

A left brace B is a matched product of left ideals $I_1, I_2, \ldots, I_n$ if the additive group $(B, +)$ is the direct sum of these left ideals.

Of course, matched products of groups have been studied for a long time, under several different names.

Matched products of left braces arise in a natural way.

Example

Let B be a finite left brace. Let $I_1, \ldots, I_n$ be the Sylow subgroups of the abelian group $(B, +)$. Then they are left ideals of B. Hence, B is a matched product of its left ideals $I_1, \ldots, I_n$.

Theorem

Let $B_1, \ldots, B_n$ be left braces, $n \geq 2$. Let

$$\alpha^{(j,i)} : (B_j, \cdot) \longrightarrow \mathrm{Aut}(B_i, +)$$

be actions that satisfy the following two conditions:

(1) for every $i \in \{1, \ldots, n\}$, $\alpha^{(i,i)}$ is the lambda map of B_i;
in other words $\alpha_x^{(i,i)}(y) = xy - x$ for $x, y \in B_i$,

(2) $\alpha_b^{(j,k)} \alpha^{(i,k)}_{\alpha^{(j,i)}_{b-1}(a)} = \alpha_a^{(i,k)} \alpha^{(j,k)}_{\alpha^{(i,j)}_{a-1}(b)}$,
for all $a \in B_i, b \in B_j$ and all $i, j, k \in \{1, \ldots, n\}$, where
$\alpha_a^{(i,j)} = \alpha^{(i,j)}(a)$
("compatibility of actions")

Theorem continued

Then there exists a (unique) structure of a left brace on $B_1 \times \cdots \times B_n$ *such that*

i) $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$
for all $a_i, b_i \in B_i$ *and* $i = 1, \ldots, n$,

ii) $\lambda_{(0,\ldots,0,a_i,0,\ldots,0)}(0, \ldots, 0, b_i, 0, \ldots, 0) =$
$(0, \ldots, 0, \alpha_{a_i}^{(i,j)}(b_j), 0, \ldots, 0)$,
for all $a_i \in B_i, b_j \in B_j$ *and* $i, j \in \{1, \ldots, n\}$.

Moreover, every $\{0\} \times \cdots \times \{0\} \times B_i \times \{0\} \times \cdots \times \{0\}$ *is a left ideal of this left brace.*

This left brace is denoted by $B_1 \bowtie \cdots \bowtie B_n$ and it called the matched product of left braces $B_1, \ldots, B_n$, defined by the actions $\alpha^{(i,j)}$.

Simple left braces arising from matched products

Hegedűs introduced the following construction of a left brace, in the context of regular subgroups of the affine group.

Let p be a prime and let n be a positive integer. Also, choose:
Q - a non-degenerate quadratic form over $(\mathbb{Z}_p)^n$,
f - an element of order p in the orthogonal group determined by Q, and define:

$$q(\vec{x}, \mu) = \mu - Q(\vec{x}) \quad (\text{here } \mu \in \mathbb{Z}_p, \vec{x} \in (\mathbb{Z}_p)^n)$$
$$b(x, y) = Q(\vec{x} + \vec{y}) - Q(\vec{x}) - Q(\vec{y}).$$

The left brace $H(p, n, Q, f)$ with additive group $(\mathbb{Z}_p)^{n+1}$ is defined via the lambda map:

$$\lambda_{(\vec{x},\mu)}(\vec{y}, \mu') := (f^{q(\vec{x},\mu)}(\vec{y}), \mu' + b(\vec{x}, f^{q(\vec{x},\mu)}(\vec{y})))$$

Let $n > 1$ be an integer and let $p_1, \ldots, p_n$ be different odd prime numbers. Let $H_i = H(p_i, n_i, Q_i, f_i)$ be a left brace of Hegedűs, for $i = 1, \ldots, n$. For every $1 \leq i < n$ suppose that c_i is an element of order p_{i+1} in the orthogonal group determined by Q_i, and c_n is an element p_1 in the orthogonal group determined by Q_s, such that $f_i c_i = c_i f_i$ for every i. For $1 \leq i, j \leq n$ such that $i \neq j$ define the maps

$$\alpha^{(i,j)} : (H_i, \cdot) \longrightarrow \mathrm{Aut}(H_j, +) : (\vec{x}_i, \mu_i) \mapsto \alpha^{(i,j)}_{(\vec{x}_i, \mu_i)},$$

with

$$\alpha^{(k+1,k)}_{(\vec{x}_{k+1}, \mu_{k+1})}(\vec{x}_k, \mu_k) = (c_k^{q_{k+1}(\vec{x}_{k+1}, \mu_{k+1})}(\vec{x}_k), \mu_k), \text{ for } 1 \leq k < s,$$
$$\alpha^{(1,s)}_{(\vec{x}_1, \mu_1)}(\vec{x}_s, \mu_s) = (c_s^{q_1(\vec{x}_1, \mu_1)}(\vec{x}_s), \mu_s),$$

and $\alpha^{(i,j)}_{(\vec{x}_i, \mu_i)} = \mathrm{id}_{H_j}$ for the remaining pairs (i, j).

Theorem (Bachiller, Cedó, Jespers, O.)

With the above notation, if $\alpha^{(i,i)} : (H_i, \cdot) \longrightarrow \mathrm{Aut}(H_i, +)$ *denotes the lambda map of* H_i*, then*

$$\alpha_b^{(j,k)} \alpha^{(i,k)}_{\alpha^{(j,i)}_{b^{-1}}(a)} = \alpha_a^{(i,k)} \alpha^{(j,k)}_{\alpha^{(i,j)}_{a^{-1}}(b)}$$

for all $a \in H_i, b \in H_j$ *and all* $i, j, k \in \{1, \ldots, n\}$*. Therefore, the maps* $\alpha^{(i,j)}$*, with* $1 \leq i, j \leq n$*, define a matched product of left braces* $H_1 \bowtie \cdots \bowtie H_n$*.*

Theorem (Bachiller, Cedó, Jespers, O.)

With the above notation, the matched product $H_1 \bowtie \cdots \bowtie H_n$ *of left braces defined via the lambda maps* $\alpha^{(i,j)}$ *is a simple left brace if and only if* $c_i - \mathrm{id}$ *is an automorphism for every* $i \in \{1, \ldots, n\}$.

Note: concrete examples of braces of this type can be constructed.

Asymmetric product and simple braces

Theorem (Catino, Colazzo, Stefanelli)

Let T and S be two left braces. Let $b\colon T \times T \longrightarrow S$ be a symmetric bilinear form on $(T,+)$ with values in $(S,+)$, and let $\alpha\colon (S,\cdot) \longrightarrow \mathrm{Aut}(T,+,\cdot)$ be a homomorphism of groups such that

$$\lambda_s(b(t_2,\ t_3)) = b(\alpha_s(t_2),\ \alpha_s(t_3)),$$
$$b(t_2,\ t_3) = b(\lambda_{t_1}(t_2),\ \lambda_{t_1}(t_3)),$$

where $\alpha_s = \alpha(s)$, for all $s \in S$ and $t_1, t_2, t_3 \in T$. Then the addition and multiplication on $T \times S$ given by

$$(t_1, s_1) + (t_2, s_2) = (t_1 + t_2,\ s_1 + s_2 + b(t_1, t_2)),$$
$$(t_1, s_1) \cdot (t_2, s_2) = (t_1 \cdot \alpha_{s_1}(t_2),\ s_1 \cdot s_2),$$

define a structure of left brace on $T \times S$. We call this left brace the asymmetric product of T by S (via b and α) and denote it by $T \rtimes_o S$.

The original construction of $T \rtimes_\circ S$ was given under a weaker assumption saying that b is a symmetric 2-cocycle on $(T, +)$ with values in $(S, +)$, but we only use the special case described above.

Note that the subset $T \times \{0\}$ is a normal subgroup of $(T \rtimes_\circ S, \cdot)$, and $\{0\} \times S$ is a left ideal of $T \rtimes_\circ S$.

Theorem (Bachiller, Cedó, Jespers, O.)

Let S be a simple non-trivial left brace. Let T be a trivial brace and let $T \rtimes_\circ S$ be an asymmetric product of T by S via $b\colon T \times T \longrightarrow S$ and $\alpha\colon (S, \cdot) \longrightarrow \mathrm{Aut}(T, +)$.
Suppose that for every $t \in T \setminus \{0\}$ there exists $t' \in T$ such that $b(t, t') \neq 0$. Then $T \rtimes_\circ S$ is simple if and only if $\sum_{s \in S} \mathrm{Im}(\alpha_s - \mathrm{id}) = T$.

Wreath products of braces

Let G_1 and G_2 be left braces. Recall that the *wreath product* $G_2 \wr G_1$ of the left braces G_2 and G_1 is a left brace which is the semidirect product of left braces $H \rtimes G_1$, where

$$H = \{f \colon G_1 \longrightarrow G_2 \mid |\{g \in G_1 \mid f(g) \neq 1\}| < \infty\}$$

is a left brace with the operations

$$(f_1 \cdot f_2)(g) = f_1(g) \cdot f_2(g)$$
$$(f_1 + f_2)(g) = f_1(g) + f_2(g)$$

for all $f_1, f_2 \in H$ and $g \in G_1$, and the action of $(G_1, \cdot)$ on H is given by the homomorphism $\sigma \colon (G_1, \cdot) \longrightarrow \mathrm{Aut}(H, +, \cdot)$ defined by $\sigma(g)(f)(x) = f(g^{-1}x)$, for all $g, x \in G_1$ and $f \in H$.

Simple braces of arbitrary derived length

Using a combination of the wreath product construction and the asymmetric product construction one proves the following result.

Theorem (Bachiller, Cedó, Jespers, O.)

For every $n \geq 1$ there exists a simple left brace B such that the derived length of its multiplicative group is $n+1$.

One defines recursively two series of left braces G_j and $\overline{G}_j$, for $j = 1, \ldots, n$, in such a way that $\overline{G}_j$ is defined as a quotient of G_j and G_j is defined as a wreath product $G_j = F_j \wr \overline{G}_{j-1}$ for some left brace F_j.

The construction yields that $|\overline{G}_n| = p_1 p_2^{m_2} \cdots p_n^{m_n}$, for some positive integers $m_2, \ldots, m_n$, where primes $p_1, \ldots, p_n$ are such that p_j is a divisor of $p_i - 1$ for all $2 \leq j \leq n$ and all $1 \leq i < j$. The existence of such primes is a consequence of Dirichlet's Theorem on arithmetic progressions.

Let A be the trivial brace $\mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n}$.

One can introduce some action of A on $\overline{G}_n$ and a symmetric bilinear form $b : \overline{G}_n \times \overline{G}_n \longrightarrow A$ in order to apply the asymmetric product construction to the braces $\overline{G}_n$ and A. Then let $B = \overline{G}_n \rtimes_\circ A$.

The wreath product construction allows to control the derived length of the constructed brace.

Factoring certain "obvious" ideal from the brace G_n, leading to $\overline{G}_n$, is necessary in order to overcome an obstruction for the simplicity of $G_n \rtimes_\circ A$.

The final asymmetric product construction $\overline{G}_n \rtimes_\circ A$ allows then to prove that this brace is simple.

All previously known simple left braces have derived length not exceeding 3.

Further results:

- More constructions of simple left braces via the asymmetric product construction.
- Interpretation of all previously constructed simple left braces as asymmetric products.

Some open problems:

1. Describe finite left braces $(B, +, \cdot)$ of order p^n for a prime p.

2. Describe the automorphism group $\mathrm{Aut}(B, +, \cdot)$ of every such brace.

3. Given two distinct primes p, q, for which positive integers m, n there exists a simple left brace B of order $p^m q^n$?